Who's fingerprints, and with what flavour, would you like today?

Svantesson, Dan Jerker B

Published in:
Privacy Law and Policy Reporter

August 2005

Who's fingerprints, and with what flavour, would you like today?

Dan Jerker B. Svantesson
Bond University, dan_svantesson@bond.edu.au

Who's fingerprints, and with what flavour, would you like today?

Dr Dan Jerker B. Svantesson

Assistant Professor, Faculty of Law Bond University

The spread of the use of biometrics has been explosive. Fingerprints, for example, are being used for a range of purposes, such as for controlling access into buildings and for logging onto computers. Furthermore, there are plans to incorporate fingerprint technology in mobile phones. In addition, the US has put pressure on the 27 countries covered by its visa waiver program to begin issuing passports with biometric identification information. Until recently, two Swedish schools even used fingerprint technology to ensure that only students who were entitled to the lunch provided could access it. There simply seem to be no end to the uses to which fingerprint technologies can be put.

However, there are several reasons to think that too much faith is being placed in these technologies. The technologies using fingerprints as identification are not completely accurate, and there are ways to fool the fingerprint readers currently in use.

Making an artificial fingerprint

The Swedish Data Inspection Board's publication *DIrekt*, recently reported how Marie Sandström[1] , a technology student at Linköping Institute of Technology, set out to verify Tsutomo Matsumoto's method of making false fingerprints. Her approach was both interesting and surprisingly simple.

Using the same method applied for decades by the police, she obtained a fingerprint of one of her colleagues; To illustrate how easily someone can copy your fingerprint, the fingerprint was obtained from a piece of glass (how many glass surfaces have you touched today?). A soot mixture was carefully applied to the fingerprint, which allowed the print to be lifted onto a white paper using adhesive tape. The fingerprint was subsequently photographed and digitally enhanced using imaging software. The finished print was then ready to be transferred onto a gelatine solution (similar to materials used in the manufacturing of some forms of "gummy-like" candy, which actually means that you could flavour the artificial fingerprint!) and the artificial fingerprint was complete.

Testing the artificial fingerprint

To evaluate the efficiency of her "product", Sandström performed tests comparing her colleagues genuine fingerprint with her gelatine fingerprint copy, on nine different fingerprint recognition systems at the CeBIT trade fair in Hannover, Germany. All systems were fooled:

The mean value of the success rate [the rate at which successful verifications or identifications are made compared to the total number of trials] using real fingerprints was 90%, and the mean values of the FAR [False Acceptance Rate] with artificial fingerprints were [...] 86% [in the second round of experiments which achieved the best results][2]

What can we learn from this?

The fact that it is possible to copy and use another persons fingerprints must be taken seriously. Even leaving aside the enormous implications this has in relation to forensic evidence, this is a

great cause for concern. While it seems clear that, it is unlikely that we will witness a widespread use of artificial fingerprints to access computers or free school lunches, it is necessary to question whether it is justified to invest large amounts of money and resources in developing fingerprint scanners as a means of ensuring a higher level of security in our society.

The evaluation of whether such investments are justified must always involve the balancing of the security benefits on the one hand, and the impact on the fundamental human right of privacy on the other. In light of the possibility of making artificial fingerprints, the security benefits may not necessarily be as great as previously though. The privacy implications, however, remain as serious.

• This short article is loosely based on an article published, in Swedish, in the Swedish Data Inspection Board's publication DIrekt #1/2005.

• Assistant Professor, Faculty of Law Bond University, Gold Coast Queensland 4229 Australia, Ph: +61 7 5595 1418, E-mail: Dan_Svantesson@bond.edu.au, (www.svantesson.org) - Research Associate, Baker & McKenzie Cyberspace Law and Policy Centre - Contributing Editor, World Legal Information Institute (www.worldlii.org) - National Convener, International Law Interest Group (Australasian Law Teachers Association) - National Rapportuer (Australia) Data Protection Research and Policy Group, (The British Institute of International and Comparative Law).

[1] She undertook her study as part of her degree at Linköping Institute of Technology and her work is available, in English, at: http://www.ep.liu.se/exjobb/isy/2004/3557/exjobb.pdf.

[2] Marie Sandström, *Liveness Detection in Fingerprint Recognition Systems* (Linköping Institute of Technology, Institutionen för systemteknik) 2004-06-04, LITH-ISY-EX-3557-2004, at 73.